PMAT 315 ASSIGNMENT 2 SOLUTIONS

1. (a) Let $n \geq 3$ be an integer, and consider the transposition

$$(12) = \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{bmatrix}$$

in the symmetric group S_n. Suppose that some permutation $\sigma \in S_n$ satisfies $\sigma(12) = (12)\sigma$. Find all possible values of $\sigma(1)$ and $\sigma(2)$.

(b) Use part (a) to describe all elements of the centralizer $C((12))$ of the element (12) of S_n, $n \geq 3$. [See the definition on page 66.]

(c) Page 114 #46.

1. (a) Suppose that $\sigma(1) = a$ and $\sigma(2) = b$, where $a, b \in \{1, 2, \dots, n\}$ and $a \neq b$ (since σ is one-to-one). Then $\sigma(12)(1) = \sigma(2) = b$ and $(12)\sigma(1) = (12)(a)$. Since $\sigma(12) = (12)\sigma$, we must have $b = (12)(a)$. But

$$(12)(a) = \begin{cases} 2 & \text{if } a = 1 \\ 1 & \text{if } a = 2 \\ a & \text{otherwise} \end{cases}$$

so since $a \neq b$ we must have either $a = 1$ (in which case $b = 2$), or $a = 2$ (in which case $b = 1$). So either

(i) $\sigma(1) = 1$ and $\sigma(2) = 2$ (which happens when $\sigma = \varepsilon$ for example), or

(ii) $\sigma(1) = 2$ and $\sigma(2) = 1$ (which happens when $\sigma = (12)$ for example).

(b) $C((12)) = \{\sigma \in S_n \mid \sigma(12) = (12)\sigma\}$. We know that if $\sigma \in C((12))$ then σ satisfies either (i) or (ii) in part (a). In fact, any permutation $\sigma \in S_n$ satisfying (i) or (ii) will be in $C((12))$, because:

- if $\sigma \in S_n$ satisfies (i), then for all $x \in \{1, 2, \dots, n\}$,

$$\sigma(12)(x) = \left\{ \begin{array}{ll} \sigma(2) = 2 = (12)\sigma(1) & \text{if } x = 1 \\ \sigma(1) = 1 = (12)\sigma(2) & \text{if } x = 2 \\ \sigma(x) & \text{otherwise} \end{array} \right\} = (12)\sigma(x);$$

- if $\sigma \in S_n$ satisfies (ii), then for all $x \in \{1, 2, \dots, n\}$,

$$\sigma(12)(x) = \left\{ \begin{array}{ll} \sigma(2) = 1 = (12)\sigma(1) & \text{if } x = 1 \\ \sigma(1) = 2 = (12)\sigma(2) & \text{if } x = 2 \\ \sigma(x) & \text{otherwise} \end{array} \right\} = (12)\sigma(x).$$

Thus $C((12))$ is exactly all permutations $\sigma \in S_n$ satisfying (i) or (ii).

(c) $Z(S_n) = \{\sigma \in S_n \mid \sigma\tau = \tau\sigma \ \forall \tau \in S_n\}$. We already know that the identity element $\varepsilon \in S_n$ is in $Z(S_n)$. Suppose that some $\sigma \neq \varepsilon$ also lies in $Z(S_n)$. Then $\sigma(i) \neq i$ for some $i \in \{1, 2, \dots, n\}$. Say that $\sigma(i) = j$ where $j \neq i$. Consider the transposition (jk) where $k \in \{1, 2, \dots, n\}$ is different from i and j (possible since $n \geq 3$). Since $\sigma \in Z(S_n)$, $\sigma(jk) = (jk)\sigma$. But $\sigma(jk)(i) = \sigma(i) = j$ while $(jk)\sigma(i) = (jk)(j) = k \neq j$, which is a contradiction. Therefore $Z(S_n) = \{\varepsilon\}$.

2. Let the *mattress group* M be the group of symmetries of a mattress, as given in problem 3 of Assignment 1. [*Note*: M has only **four** elements. See the solution posted on the course website.]

(a) Is $M \approx \mathbb{Z}_4$? Explain.

(b) Use the construction in the proof of Cayley's Theorem to find four permutations of a four-element set which form a group isomorphic to M.

2. (a) No, $M \not\approx \mathbb{Z}^4$, because $\mathbb{Z}_4$ is cyclic while M cannot be cyclic because it has no elements of order 4.

(b) Using the notation in the solution of Assignment 1 problem 3, $M = \{E, R, L, S\}$, and the Cayley table of M is

	E	R	L	S
E	E	R	L	S
R	R	E	S	L
L	L	S	E	R
S	S	L	R	E

.

From the proof of Cayley's Theorem, we define the following four permutations on M:

- T_E defined by $T_E(E) = E$, $T_E(R) = R$, $T_E(L) = L$, $T_E(S) = S$, so $T_E = \varepsilon$;
- T_R defined by $T_R(E) = R$, $T_R(R) = E$, $T_R(L) = S$, $T_R(S) = L$, so $T_R = (ER)(LS)$;
- T_L defined by $T_L(E) = L$, $T_L(R) = S$, $T_L(L) = E$, $T_L(S) = R$, so $T_L = (EL)(RS)$;
- T_S defined by $T_S(E) = S$, $T_S(R) = L$, $T_S(L) = R$, $T_S(S) = E$, so $T_S = (ES)(RL)$.

These form a group isomorphic to M, with the Cayley table

	T_E	T_R	T_L	T_S
T_E	T_E	T_R	T_L	T_S
T_R	T_R	T_E	T_S	T_L
T_L	T_L	T_S	T_E	T_R
T_S	T_S	T_L	T_R	T_E

.

3. Let G be a group, and define $\phi : G \to G$ by $\phi(g) = g^2$ for all $g \in G$.

(a) Is ϕ an automorphism of G for every group G? Explain.

(b) Is ϕ an automorphism of G for every Abelian group G? Explain.

(c) Is ϕ an automorphism of G for $G = (\mathbb{R}^+, \cdot)$? Explain.

3. (a) and (b) The answer in both cases is **no**, because ϕ need not be one-to-one or onto. For example, for the Abelian group $(\mathbb{Z}, +)$, ϕ would be written as $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, so the range of ϕ is all even integers, not all integers, so ϕ is not onto. Another example would be the Abelian group $(\mathbb{R} - \{0\}, \cdot)$, in which case ϕ would not be one-to-one, for example $\phi(1) = 1^2 = 1$ and $\phi(-1) = (-1)^2 = 1$, and ϕ is not onto either, because the range of ϕ is only positive real numbers.

Note that for any Abelian group G, it is true that ϕ satisfies the isomorphism property $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$, because $\phi(gh) = (gh)^2 = g^2h^2 = \phi(g)\phi(h)$. But if G is not Abelian, then this need not hold either, because $(gh)^2 = ghgh \neq ggHh = g^2h^2$.

(c) For $G = (\mathbb{R}^+, \cdot)$, which is Abelian, we do have $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{R}^+$ as above. It is also true that ϕ is one-to-one and onto:

- For any $x, y \in \mathbb{R}^+$, if $\phi(x) = \phi(y)$ it says $x^2 = y^2$, which implies $x = y$ since both x and y are positive. Thus ϕ is one-to-one.
- For any $x \in \mathbb{R}^+$, $\sqrt{x}$ is defined and in R^+ since x is positive, and $\phi(\sqrt{x}) = (\sqrt{x})^2 = x$. Thus ϕ is onto.

Therefore, **yes**, ϕ is an automorphism in this case.

4. Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and $H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$.

(a) Prove that G is a subgroup of $(\mathbb{R}, +)$.

(b) Prove that $(H, +)$ is a group, where the operation is the usual addition of matrices.

(c) Prove that $G \approx H$.

(d) Find two elements in $\mathrm{Aut}(G)$ which are not the identity automorphism.

(e) Is G cyclic? Explain.

4. (a) We'll use Theorem 3.1 on page 61. Let $r_1 = a + b\sqrt{2}$ and $r_2 = c + d\sqrt{2}$ be arbitrary elements of G, where $a, b, c, d \in \mathbb{Z}$. Then

$$r_1 - r_2 = (a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in G,$$

because $a - c \in \mathbb{Z}$ and $b - d \in \mathbb{Z}$. Since G is obviously nonempty, Theorem 3.1 implies that G is a subgroup of $(\mathbb{R}, +)$.

(b)

- H is closed under the operation: Let $M_1 = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ and $M_2 = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$ be arbitrary elements of H, where $a, b, c, d \in \mathbb{Z}$. Then

  $$M_1 + M_2 = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a + c & 2b + 2d \\ b + d & a + c \end{bmatrix} = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix}$$

  lies in H, since $a + c, b + d \in \mathbb{Z}$.
- We know already that matrix addition is associative.
- The identity element is the zero matrix $\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, which is in H by putting $c = d = 0 \in \mathbb{Z}$. Then clearly $\mathbf{0} + M = M$ for every matrix $M \in H$.
- If $M = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is an arbitrary element of H, where $a, b \in \mathbb{Z}$, then the inverse element is the negative $-M = \begin{bmatrix} -a & -2b \\ -b & -a \end{bmatrix}$, which is in H because $-a, -b \in \mathbb{Z}$.

Therefore H is a group.

Note. Alternatively, if we accept as already known that the set of all 2×2 matrices with integer entries forms a group under matrix addition, then we could just prove that H is a subgroup of this group, as in part (a).

(c) We define $\phi : G \to H$ by: for all $a, b \in \mathbb{Z}$, $\phi(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. Then ϕ is obviously one-to-one and onto. Also, for arbitrary $a, b, c, d \in \mathbb{Z}$,

$$\begin{aligned} \phi\Big((a + b\sqrt{2}) + (c + d\sqrt{2})\Big) &= \phi\Big((a + c) + (b + d)\sqrt{2}\Big) \\ &= \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \\ &= \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}). \end{aligned}$$

Therefore ϕ is an isomorphism, so $G \approx H$.

(d) Two such automorphisms are $\phi_1 : G \to G$ and $\phi_2 : G \to G$ defined by:

$$\phi_1(a + b\sqrt{2}) = -a - b\sqrt{2} \quad \text{and} \quad \phi_2(a + b\sqrt{2}) = b + a\sqrt{2}.$$

It is clear that both ϕ_1 and ϕ_2 are one-to-one and onto, and that they are not equal to each other or to the identity automorphism. Also, for all $a, b, c, d \in \mathbb{Z}$,

- $\phi_1\Big((a + b\sqrt{2}) + (c + d\sqrt{2})\Big) = \phi_1\Big((a + c) + (b + d)\sqrt{2}\Big) = -(a + c) - (b + d)\sqrt{2} = (-a - b\sqrt{2}) + (-c - d\sqrt{2}) = \phi_1(a + b\sqrt{2}) + \phi_1(c + d\sqrt{2})$, and
- $\phi_2\Big((a + b\sqrt{2}) + (c + d\sqrt{2})\Big) = \phi_2\Big((a + c) + (b + d)\sqrt{2}\Big) = (b + d) + (a + c)\sqrt{2} = (b + a\sqrt{2}) + (d + c\sqrt{2}) = \phi_2(a + b\sqrt{2}) + \phi_2(c + d\sqrt{2})$.

So ϕ_1 and ϕ_2 are indeed automorphisms.

Note. ϕ_1 is just the function $\phi(g) = -g$, which is an automorphism because G is Abelian (see Exercise 10 on page 132).

(e) No, G is not cyclic. We prove this by contradiction. Suppose that G is cyclic, say G is generated by some element $a + b\sqrt{2}$. By assumption,

$$G = < a + b\sqrt{2} > = \{k(a + b\sqrt{2}) \mid k \in \mathbb{Z}\} = \{ka + kb\sqrt{2} \mid k \in \mathbb{Z}\}.$$

Of course a and b cannot both be zero, because $0 + 0\sqrt{2} = 0$ would generate only the trivial subgroup $\{0\}$. So we have two cases:

Case (i). If $a \neq 0$, then since $0 + 1\sqrt{2} = \sqrt{2} \in G$, by assumption $\sqrt{2} = ka + kb\sqrt{2}$ for some $k \in \mathbb{Z}$. Clearly $k \neq 0$, and so since $a \neq 0$, we must have $ka \neq 0$, so $kb \neq 1$. Thus we get $(1 - kb)\sqrt{2} = ka$ and then $\sqrt{2} = \dfrac{ka}{1 - kb}$, which is impossible since $\sqrt{2}$ is irrational while $\dfrac{ka}{1 - kb}$ is rational.

Case (ii). So we must have $a = 0$, in which case we know $b \neq 0$. This time we note that $1 + 0\sqrt{2} = 1 \in G$, so by assumption $1 = ka + kb\sqrt{2} = kb\sqrt{2}$ for some $k \in \mathbb{Z}$. But then $\sqrt{2} = 1/(kb)$, which again is impossible since $\sqrt{2}$ is irrational.